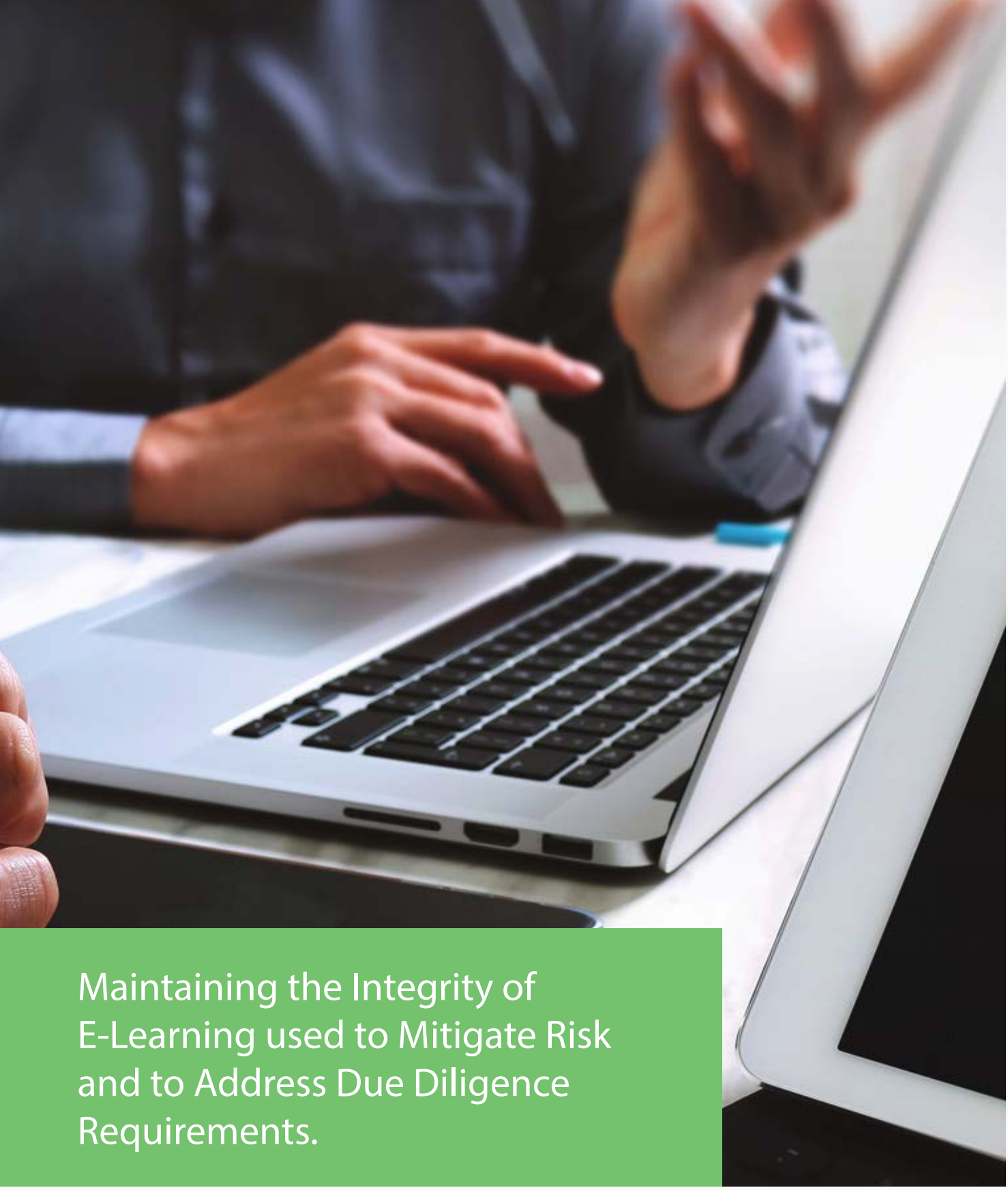


Maintaining the Integrity of E-Learning used to Mitigate Risk and to Address Due Diligence Requirements.

January 2019

IntegrityAdvocate

inegrityadvocate.com

+EXECUTIVE SUMMARY

The $200 billion-dollar e-learning industry is changing the game when it comes to workplace training and testing. It is offering organizations massive cost savings and the ability to develop personnel with an efficiency that was not feasible with traditional learning, but at the potential cost of process integrity and weakened due diligence.

Without verifying participation and verifying user identity, organizations have no way of knowing if training is being received by those it was intended for, and no way of confirming the desired participation of the learner.

Of the various forms of identity/participation verification available on the market, no other organizations can match the same level of efficiency, mobility, privacy compliance and value as Integrity Advocate. Integrity Advocate's patent-pending technology is saving organizations millions of dollars, while ensuring due diligence and process integrity.

+TABLE OF CONTENTS

Executive Summary 2

Introduction 4

E-Learning: Anytime, Anywhere, At What Cost? 5

The Problem of Proof, Cheating and Impatience 9

Rising to the Challenge of Legal and Regulatory Requirements 11

Identity and Integrity Verification that Works 14

Case Study: Suncor Fort Hills Site 15

Conclusion 16

More Information 18

+INTRODUCTION

The online learning revolution is here, and it is a rapidly growing and ever-changing juggernaut. In 2018 the e-learning market was worth an enormous $190 billion globally[1] , with compound annual growth rate of 7%.

While businesses around the globe look for ways to lower costs and increase worker competency and productivity, e-learning has provided opportunities for personnel development on a flexible schedule at a low cost, often requiring no more than a phone and an internet connection.

Doing away with on-site, or classroom, learning saves money, but also raises significant due diligence and legal issues for organizations. How do you tell though a computer screen that someone is who they say they are? How do you tell if the person participated fully? If a legal issue arises, how do you prove your organizational due diligence?

With the rise of e-learning, there has also been an inevitable rise in unethical learner behavior. A 2012 survey of onlinecollege.org students revealed that 73% admit to engaging in 'deceit' while participating in e-learning activities, compared to 53% of students who admitted to 'deceit' while in a traditional learning environment[2]. It is reasonable that learners may be more cavalier in an on-line environment and act in a manner that would not be seen as acceptable in an instructor-led learning environment.

A reasonably practicable solution is needed. Something that ensures e-learners are who they say they are, that they participate as required, provides sufficient records for legal purposes and prevents unethical behaviors, without compromising the flexibility and economical value that makes online training and testing such an effective business tool. The solution is Integrity Advocate, a mobile-friendly, browser-agnostic, privacy-protected technology that both verifies learner identity and their participation throughout the elearning event.

+ E-LEARNING: ANYTIME, ANYWHERE, AT WHAT COST?

The term e-learning is believed to have been coined in 1998, but was first defined in 1999 at a CBT Seminar in Los Angeles, California, as "a way to learn based on the use of new technologies allowing access to online, interactive and sometimes personalized training through the internet or other electronic media (intranet, extranet, interactive TV, CD-ROM etc.) so as to develop competencies while the process of learning is independent from time or place."[3]

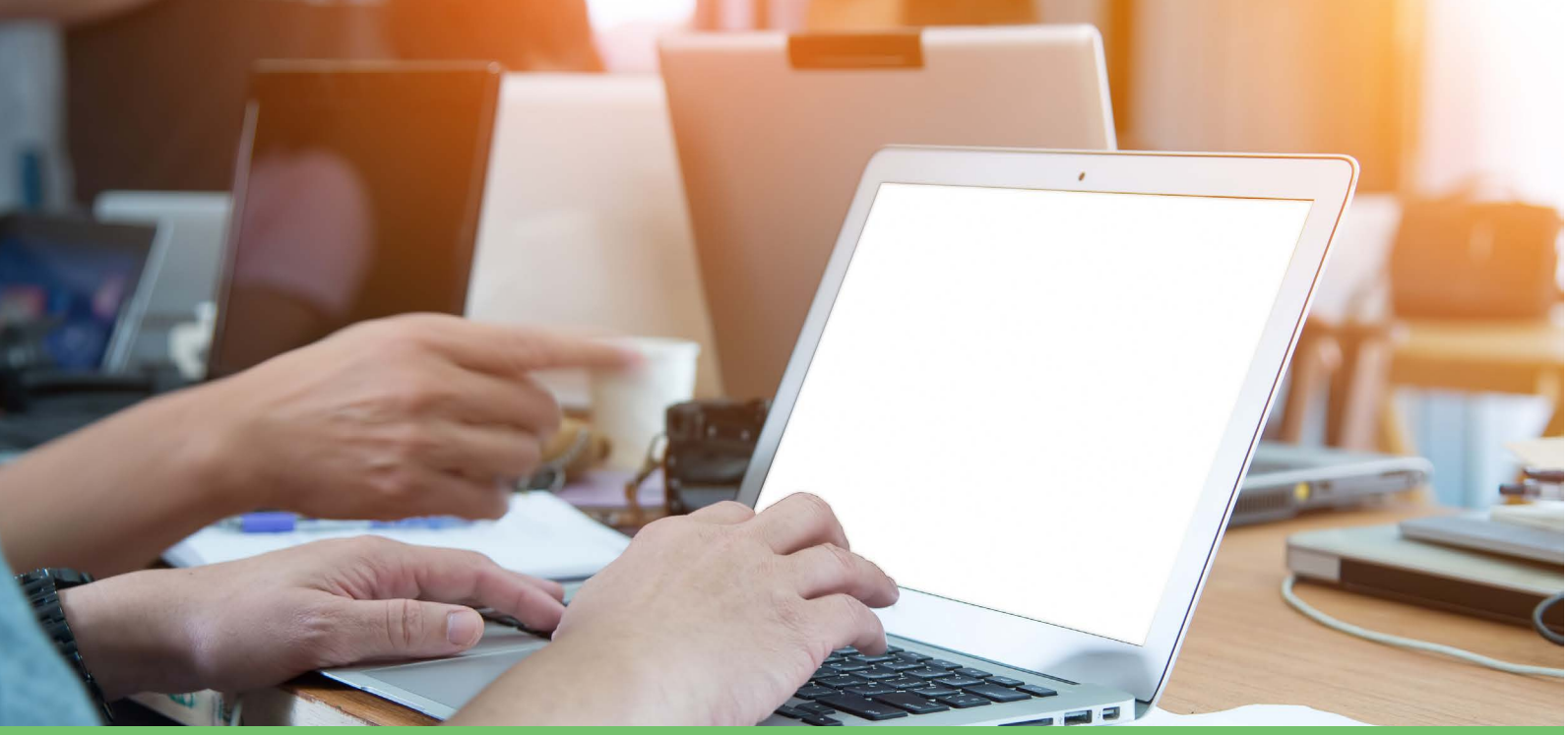
More than 20 years later, e-learning is a multi-billion-dollar industry that has more than doubled in value in the last five years alone. While e-learning is applicable across a wide variety of industries, from governments and post-secondary institutions, to professional organizations, it has made some of it's biggest impact in the business world.

The switch to e-learning to provide training means that minimal resources are needed (compared to instructor-led training), no matter the number of employees taking the training. Traditional instructor-led training has significant associated costs that range from dedicated physical spaces, and materials to instructors and support staff that are no longer necessary or relevant with e-learning where personnel can take training as their schedule permits, without having the potential cost of travel to a training location, even without having to be at the office. It also decreases the amount of time personnel spend completing training, a Brandon-Hall Study showed that e-learning, on average, uses 40-60% less employee time than traditional learning[4]. Online training also allows for better access to translation and aid services, allowing training to be quickly and easily customized for those with learning disabilities or ESL requirements with a significantly lower cost than traditional training.

E-Learning also aids in worker retention, efficiency and productivity. It is estimated that 40% of workers who do not receive training will leave their job within the first year if they feel that they have not been developed sufficiently for the position they are in[5].

An IBM Case Study from 2013 showed that the switch to e-learning saved their company approximately $200 million[6]. They estimated that every dollar they invested in e-learning represented a $30 increase in productivity as personnel could apply their skills more immediately than with traditional training. IBM also noted in their case study, a belief that personnel could learn and retain larger amounts of knowledge using e-learning than they had previously seen with more traditional training techniques.

In addition to training as a development tool, many industries also require additional specialized training and orientations relating to jurisdictional, legislative and/or safety regulations. The education, medical and legal professions also stress webinars as important development tools for busy industry professionals, as they can access the content from almost anywhere, at any time.



While e-learning has many advantages that seem to make traditional learning a thing of the past, it does have one glaring downfall. Where traditional learning techniques allow for a supervisor, educator or proctor to monitor individual participation, e-learning is done at a distance behind the, often-anonymous, screen of a computer. This raises the issue of proof for many companies attempting to comply with due diligence requirements and/or wanting the intended benefits of an informed and/or competent workforce.

The most recent statistics available from the Association of Workers' Compensation Boards of Canada[7] and the United States Bureau of Labor Statistics[8] show more than 3 million workplace incidents occurred in 2015 alone. Investigation of these incidents by the respective governing bodies focuses on key factors that may have prevented the incident from occurring and focus on whether an employer demonstrated an appropriate level of due diligence to prevent the incident, including providing and ensuring the completion of appropriate awareness and competency development training for effected personnel. Occupational Safety and Health Association (OSHA) investigators are trained that the first question to be asked in the case of a workplace incident is whether personnel received adequate training to do their job[9].

With safety performance becoming an important differentiator for many employees and their organizations, proof problems are not likely to end anytime soon. Without a valid form of identity verification, some organizations will not recognize online training as being completed, even with records of training being provided. Landmark cases such as R. v. Rose's Well Services Ltd.[10] , where an employee admitted to taking the training for other employees, have shown that employers need to do more than just provide training, they must also prove who completed and/or participated in the training.

While some organizations have chosen to develop e-learning with the requirement of individual logins and regular 'click' requirements to necessitate human involvement there is nothing integral in this that ensures that the pages, videos or animation is being watched and not just played. The general anonymity of un augmented e-learning means there is also no method to create a valid record showing that the individual the training was provided for, was the one who participated in the training according to the standards of the organization (i.e. adhered to the organizations expectations of ethical behaviour).

+ E-LEARNING AS A CRITICAL CONTROL AND LEGAL REQUIREMENT

All occupational health and safety legislation in jurisdictions across North America require three levels of controls to be used according to a hierarchy of their effectiveness (engineering then administrative then personal protective equipment). Training is not only a universally used administrative control, but it is also is used to address the 'right to know' requirements integral to the same legislation. For these reasons organizations uses training and orientations extensively to mitigate the variety of risks associated with utility strikes, confined space entries, working at heights, administering first aid, hazardous material spill response, emergency response, asbestos handling, equipment operation, etc.

Note: Sadly, numerous public safety organizations have not yet taken the steps to verify the identity and participation of learners where e-learning is used as the primary preventative measure for issues that range from child sexual abuse, violence in sport, boater safety to over-serving of alcohol, marijuana sales.

Both regulators and the Courts have clearly expressed that employers are expected to take all reasonably practicable efforts to use technological improvements that are reasonable in their cost and the effort required to implement and manage. In the case of online training, the Industrial Occupational Safety and Health Council states, in a 2015 best practice that; "Organizations which fail to adopt technological advancements that are readily available and economical, are vulnerable to breaching the hierarchy of control measures."[11]

Although professional organizations such as International Association for Continuing Education and Training (IACET) and the Chartered Professionals in Human Resources (CPHR) have drawn attention to, provided warnings about, and directed organizations to published guidance on the necessity of identity and participation verification when using e-learning for regulatory compliance and risk mitigation, unverified e-learning still occurs. Industry organizations are now creating member awareness in light of the regulatory interpretations and specific regulatory changes that have come to pass. Examples of both include, but are not limited to;

Alberta Government (OHS Enforcement), Canada

"An online course that does not identify the participant does not meet the minimum standard." #10114935

"The training agency should not be providing proof of training for students they cannot verify completed the course." #16874685

New York City, USA Legislation (OSHA Enforcement)

"only in-person training and actively proctored online training will be accepted"

Ontario, Canada Ministries Prevention Office (OHS Enforcement)

"Training providers are responsible for ensuring the identity of their learners, and they will continue to be required to validate learner identity in any fully online course"

OSHA, USA (OHS Enforcement)

Employers must be able to show both that the training was adequate, based on training content, and that the employee received the training." #2254-09R 2015

Canadian Association of Petroleum Producers (CAPP): Industry Association

"It is vital that employers can verify that the intended personnel received the online training, and that they participated in it as intended."

Industrial Occupational Safety and Health Alberta: Industry Organization

"ID verification and Proctoring technology is particularly critical when organizations use web-enabled educational materials as part of risk control strategies" IOSH Alberta

American National Standards Institute (ANSI) and the American Society of Safety Professionals

6.1.3 Each trainee,, being evaluated shall be properly identified. *ANSI+ASSE Z490.1*

7.2.2 Delivery records for each training event shall identify the trainees participation in the training *ANSI+ASSE Z490.1*

+ THE PROBLEM OF PROOF AND UNETHICAL BEHAVIOR

Whether e-learning is conducted to develop personnel and increase retention, or as part of legal requirements, e-learning affords cost and productivity savings traditional learning does not, but it must have some form of integrity verification to prevent proof problems, and undesirable learner behaviors (both unintended and overtly unethical) that compromise the legal standing of organizations.

Learner substitution, or the impersonation of others, is one of the most prevalent forms of undesirable learner behavior. This can range from someone other than the user advancing the training when the learner is absent to a learner providing someone else with their login information to take the entire test or training for them. This type of behavior seems most prevalent in situations where client training and/or regulatory requirements must be completed before work, such as completing site orientations, permit receiver, ground disturbance and/or chemical safety training. Since these types of training, when delivered on-line are often easily done by admin personnel (entry-level content, basic end-of-training testing), and can be seen as repetitive, unnecessary and redundant by the intended personnel, learner substitution, or the impersonation is not interpreted by learners as 'unethical'. Organizations have attempted to address this by requiring the use of usernames, passwords, tokens or by requiring users to check off an affirmation of their willingness to comply with participation expectations.

Such precautions have not been able to prevent the intended user from providing their login credentials to someone else, thus the actual identity of intended participation of the intended learner is unverifiable.

In cases where identity is confirmed by submission of a photo ID, or some other method, users can still succumb to their own impatience or disinterest, switching out with someone else, or leaving entirely after their identity has been confirmed. In most e-learning scenarios there is nothing in place to confirm participation throughout the learning event.

+USER IDENTIFICATION METHODS IN USE

To establish learner identity, some e-learning companies are incorporating a variety of identity verification tools aimed at increasing the integrity of e-learning and removing proof problems. These forms of identity verification can be broken down into three types of identification proxies; two-step identification, personal information and biometrics.[12]

Two-step identification proxies are the most common, and perhaps the most broken of the methods currently in use. Two-step identification proxies involves the use of a unique username and password to access content and 'prove' identity, like logging in to an email account. What this type of 'verification' does not account for, is that users can, and do, share their username and password with others or login themselves, then have another person take the e-learning on their behalf.

In an attempt to counter some of the issues with two-step identification proxies, some learning management systems offer time-sensitive codes that are in addition to the username and password, while others may require a cell phone number be attached so that they may send you special access codes that are frequently updated. Although the complexity of the login process can make password hacking more difficult for third-parties, it does not verify the identity of a user accessing the e-learning because a password, username and tokens are easily shared with others, it also does nothing to improve a learners motivation to participate in their session as intended.

The use of additional personal information is another attempt at identity verification. This method is similar to two-step identification, which requires users to use a username, a passcodes and instead of a token the user must enter private information such as place of birth, mother's maiden name, Social Insurance Number or driver's license number. The logic behind the use of this type of verification is that a user's identity is more assured because the user is less likely to share that type of information with others out of concern for identity theft. This type of verification comes with additional security and privacy issues, as it requires the user to share personal information (i.e. SIN, driver's license number), with the same e-learning provider that also holds their phone number, home address, employer etc. The combination of governmental records and personal information within one system creates an unnecessary privacy risk for the user. Additionally, this type of verification again relies on the participants desire to not share their information with others.

Finally, there is the use of biometrics in the identification process, which can range from facial detection to fingerprint recognition and/or retina scans. Arguably the best form of identity verification as biometrics are not easily transferred to another person. The challenge in using many forms of biometrics for identity verification is that they often require the use of specific equipment, such as fingerprint scanner or high definition cameras, that are not consistently available. Unfortunately, most types of biometrics work only at the point of log in, and do not continually monitor session to ensure that a user does not leave during the session, or having another user answer in their place.

Note: the methods of identity and participation verification discussed up to this point did not include the multitude of proctoring companies that exist designed to serve the post-secondary education market due to the fact that the technological solutions they provide are incompatible with modern eLearning delivering and accessibility needs. These legacy proctoring technologies require a combination of the following; specific browsers, plugins and/or software installed, users to schedule their training events in advance, the necessity to use a desktop computer (no mobile devices), administrative rights to the computer, robust privacy mitigation and support efforts due to the abundance of personal information collected and shared about the user, their environment and the computer used to access the eLearning.

+ RISING TO THE CHALLENGE OF LEGAL AND REGULATORY REQUIREMENTS

In a traditional instructor-led learning environment, the instructor would verify the identity and participation of users throughout a session, by checking ID at the start of the session (when not known to the instructor), and visually monitoring them throughout to ensure individuals do not leave, sleep, or engage in unethical behaviour. Outside of the traditional learning environment, an individual's identity is most commonly verified for things such as legal document signing, by using a third-party service such as going to a Notary Public or Commissioner of Oaths. This process verifies identity through an individual meeting with a notary or commissioner and having their name and facial characteristics matched to that of their government issued photo identification.

The verification of learner identity and participation in e-learning events should (if the events are to have the same integrity, impact, and value) be managed in a manner to that of the same instructor-led events. The process developed and provided by Integrity Advocates has combined the legal acceptability of a notary or commissioner, the proctoring standard of instructor-led learning and the highest possible level of biometric technology possible utilizing the technological capability inherent in the vast majority of user devices (desktops, laptops, tablets and mobile phones).

Biometric Identification technology becomes more widespread every day. Apple, Samsung, Google and Windows, are just a small number of major technological companies who are incorporating biometric identification into all their products. Whether it is the fingerprint scanners of iPhones and Pixels, to the retina scans of the new Samsung phones and the facial recognition logins on Windows 10, biometrics is becoming common place for many people.

A survey conducted by Visa Europe showed that 69% of millennials believed that biometrics identity verification would offer a faster and safer than PIN numbers and passwords[13]. A survey of 4,000 United Kingdom and United States consumers also showed the appetite for new forms of identity verification, with 52% saying that they would choose anything over a traditional username and password. 20% of those stated a preference for biometric identification.[14]

While other types of online proctoring are available, they come with a high cost and requirement for additional software and/or hardware to work, as well as pre-scheduling e-learning sessions within specific time frames[15] . The Integrity Advocate application is on demand, functioning 24/7/365, eliminating the need for scheduling. Integrity Advocate harnesses the existing technological capabilities of a user's web browser and computer, avoiding the need for installation of third-party software or administrative privileges on the computer being used to access the e-learning.

Not only are the individuals using the Integrity Advocate application as part of their e-learning experience, not required to install software on their systems, but the organizations that integrate Integrity Advocate into their e-learning can do so by adding a single line of code. Using biometrics, automation and non-invasive technology, the associated operating costs and market cost of the Integrity Advocate application is 60-80% lower than other software based systems.

Psychological studies also show, that even if identity verification were not an issue, there is a benefit to having users knowing they are being monitored during training events. This phenomenon, known as the Hawthorne Effect, which states that when personnel are observed, and know they are being observed, they tend to change their behaviour, putting in more effort and adhering to expectations[16]. Since users are aware of Integrity Advocate running throughout their session, via a high visibility 'button', users are more likely to focus on the e-learning.

Integrity Advocate is customizable, economical, secure and trusted and can be applied to any web-delivered course in minutes. These attributes more than meet the 'reasonably practicable' requirements of Regulators and the Courts.

+ PRIVACY AND SECURITY PROTECTED

Personal details gathered during sessions are gathered using 256-bit encryption, the same used by major financial institutions, to keep data safe and secure. Integrity Advocate also restricts access to its application if the learner is using an insecure web browsers to protect the user from sending information online that does not meet current data security standards.

To manage privacy concerns, proctoring media and images of submitted government identification are deleted after sessions are proctored. This means that sessions where the learner has complied with participation expectations only a portrait image of the learner is retained. Where compliance with participation expectations are not met the minimum number of media frames are also retained as evidence of the violations and where necessary unnecessary personal details censored (blacked out). The Learning Management System's (LMS) using Integrity Advocate are granted access to only the aforementioned information as well as whether a participant has passed or failed the identity and integrity verification process.

Note: the above summary of how privacy concerns are managed by Integrity Advocate for the protection of the learners, third-party LMS providers, employers and associations is extensively summarized and does not explain how Integrity Advocate's use of 'Privacy by Design' allows it to achieve the highest standard of privacy protection and provide the only General Data Protection Regulation (GDPR) compliant ID and participation SAS application on the market. More information on this aspect can be provided upon request.

+ IDENTITY AND INTEGRITY VERIFICATION THAT WORKS

The gap in the market and the need for a more efficient and cost-effective form of online identification for e-learning, that would also fulfill due diligence requirements was noticed by a Canadian company whose stakeholders had the combined backgrounds in the areas of software engineering and risk management. It was from this team that Integrity Advocate was created, an online identity verification and proctoring service. In addition to the basic identity verification service, done using a combination of biometrics and government verification, Integrity Advocate also runs algorithms identifying behavior work with facial detection throughout the session to determine whether a participant is following pre-set participation rules determined by the e-learning provider

The Integrity Advocate application integrates directly into custom-built, open source and enterprise Learning Management Systems (LMS) alike. Users that log into these systems to access their assigned training do so in the manner prescribed by the LMS and only at the point of launching an eLearning course or testing does the Integrity Advocate application appear and ask the learner to permit the use of their web camera(s) and microphone. Participants are then asked to take a portrait picture of themselves as well as one of their government-issued photo identification, read the participation expectations and then trigger Integrity Advocate to shrink down the size of a button and monitor their participation until completion. Programmatically the Integrity Advocate application compares the name the learner to the name on the provided government issued ID (using optical character recognition technology) and then biometrically compares the image of the individual to the picture on their ID to validate the identity of the individual. For the ongoing monitoring of the learner, Integrity Advocate again uses biometrics to confirm that the user taking the training is the same individual that was verified against the provided ID. Further use of biometrics and facial detection technology is utilized based on the participation rules to verify such things as multiple participant, the absence of the learner as well as various unethical behaviors. Human reviewers augment the automated processes to ensure quality and to make judgement calls based on identified occurrences.

The Integrity Advocate team works continually with existing and potential integration partners to ensure that they are getting full functionality from the application. New security measures, proctoring options, and services are added regularly to keep up with the rapid changes in online security, technology and eLearning trends. Legislative and regulatory initiatives are closely monitored to ensure that Integrity Advocate always meets or exceeds due diligence requirements in any country or jurisdiction specified by clients using the software. Advanced integration and customization options are also available through one-on-one coaching with the Integrity Advocate programming team.

+ CASE STUDY: SUNCOR FORT HILLS SITE

The Suncor Fort Hills Site, located in Alberta, Canada is an excellent example of the benefits of Identification Verification with Integrity Advocate. The project, operated by the multinational Suncor Energy, will employ approximately 5,000 construction workers during peak of construction and create more than 1,600 permanent positions when production facilities are fully operational.[17]

In a released video covering the lessons learned during the design and implementation of orientation programs for the Fort Hills Site[18] , Suncor identified a savings of more than $5 million in a two-year period. This savings was due to being able to switch from instructor-led training on-site before entry onto the site, to an e-learning delivery of their orientation course.

While the benefits of switching to e-learning for this were obvious for them, cost savings from no longer having to pay for transportation to the classroom, a dedicated class space and full-time on site trainer, there were initial concerns about the lack of assurance that that people coming to the site had taken the orientation themselves, or that they had watched the entire orientation content.

They engaged stakeholders within various departments, from information and process management, to legal and learning capability, to investigate the issue and potential solutions. The review honed-in on Integrity Advocate and due to its ability to protect the integrity of the training of those coming to site, as well as supporting regulatory due diligence, the pilot implementation of the new e-learning orientation system was approved in the fall of 2014. The online orientation was later made mandatory for all visitors and workers to the Fort Hills site in 2016.

Estimates from Suncor show that the initial investment of switching from classroom to e-learning was recovered within two months and a return on investment of more than 100%[18]. Without Integrity Advocate, they would not have been able to switch to e-learning without compromising process integrity in a manner which could leave them holding a serious legal risk.

+CONCLUSION

With a 900% growth rate since 2000[19] , e-learning is here to stay. Organizations utilizing e-learning have shown that e-learning has reduced the effort required for employee development, improved personnel retention, increased revenue per employee by 26%[20] , and provided an excessively large return on investment. Sadly, for organizations, this dramatic move to e-learning also resulted in an unforeseen loss in learning integrity for topics that extended into regulatory requirements and risk mitigation.

Industry has understood for a long time that any individual asked to take a course needs to attend the course and that any organization indicating that an individual took training must actually know that the individual actually did. The move from instructor-led to online has not removed this expectation or given any logical basis for why a lower standard would be acceptable.

Are you tracking, recording or providing proof of training to individuals that you do not know completed specific training? If individuals not participating in the training is acceptable, then why have them do the training at all. Is your organizations current method of delivering e-learning meet the due diligence test?

Developed with due diligence requirements in mind, Integrity Advocate harnesses the capabilities of popular web browsers to effectively and efficiently verify both user identity and participation.

1. https://www.weforum.org/agenda/2016/09/is-online-learning-the-future-of-education/
(Retrieved 22 December

2. 2016)http://www.onlinecollege.org/2012/07/23/do-online-students-cheat-more-often/
(Retrieved 19 December 2016)

3. http://www.leerbeleving.nl/wbts/1/history_of_elearning.html
(Retrieved 5 January 2017)

4. http://info.shiftelearning.com/blog/bid/301248/15-Facts-and-Stats-That-Reveal-The-Power-Of-eLearning
(Retrieved on 16 December 2016)

5. https://www.go2hr.ca/articles/employee-training-worth-investment
(Retrieved 23 December 2016)

6. http://www.icmrindia.org/casestudies/catalogue/Human%20Resource%20and%20Organization%20Behavior/HROB030.htm
(Retrieved 20 December 2016)

7. http://awcbc.org/?page_id=14
(Retrieved 27 December 2016)

8. https://www.bls.gov/news.release/osh.nr0.htm
(Retrieved 27 December 2016)

9. https://www.osha.gov/Publications/osha2254.pdf
(Retrieved 20 December 2016)

10. http://www.globaltrainingedge.ca/wp-content/uploads/2014/09/Due-diligence-cases-details-Copy.pdf
(Retrieved 23 October 2016)

11. https://www.ioshalberta.com/web-proctoring
(Retrieved 30 December 2016)

12. https://econsultancy.com/blog/67718-key-trends-in-online-identity-verification-so-everybody-knows-you-re-a-dog/
(retrieved 10 January 2017)

13. https://www.visaeurope.com/newsroom/news/generation-z-ready-for-biometric-security-to-replace-passwords
(retrieved 3 January 2017)

14. http://www.iotevolutionworld.com/iot/articles/421522-more-than-half-consumers-want-biometrics-instead-passwords.htm
(Retrieved 21 December 2016)

15. https://library.educause.edu/~/media/files/library/2016/5/eli7133.pdf
(Retrieved 22 December 2016)

16. https://explorable.com/hawthorne-effect
(Retrieved 3 January 2017)

17. http://forthills.suncor.com/
(Retrieved 28 December 2016)

18. https://www.youtube.com/watch?v=HFf0c5O8u0A&index=3&list=WL&t=13s
(Retrieved 9 January 2017)

19. http://elmezine.epubxp.com/t/55545-elearning-april/28
(Retrieved 4 January 2017)

20. http://www.images.adobe.com/www.adobe.com/content/dam/Adobe/en/products/adobeconnect/pdfs/elearning/092111-rr-nextgen-elearning-ba-ctcrevised-vendor.pdf
(Retrieved 22 December 2016)

+ FOR MORE INFORMATION

For more information, please contact customerservice@integrityadvocate.com

IntegrityAdvocate

inegrityadvocate.com